

DATA PROCESSING AGREEMENT

Processing of personal data

In accordance with Art. 9 of the FADP (SR 235.1)

Generic template

This template is provided for guidance. Replace all the fields in square brackets [] with the information specific to your practice and your provider. Having it checked by a lawyer specialising in the field is recommended before use.

Parties to the agreement

The Processor: [Name of the IT provider], [Address, postcode, town, canton]

Represented by [Surname and first name], [Role]

The Controller: [Name of the dental practice]

Art. 1: Purpose

This agreement governs the processing of personal data carried out by [Provider] as part of its IT services, in accordance with Art. 9 FADP.

The Processor acts only on the instructions of the Controller. It processes personal data only to the extent necessary to perform the agreed services.

Art. 2: Nature of the data accessible

The following data may be accessible as part of the services:

- User names and workstation identifiers
- System metadata (status of machines, alerts, logs)
- Passwords for access to the practice's systems
- Administrative documents sent to the provider
- [Other categories depending on your situation]

No medical data, X-rays or patient files are collected, stored or processed by [Provider].

Art. 3: Purpose of the processing

The accessible data is used exclusively for the following purposes:

- Preventive and corrective maintenance of IT systems
- Security monitoring
- Management of access and passwords on behalf of the practice
- Data backup and restore
- [Other purposes depending on your services]

No data is processed for any other purpose, sold, or disclosed to third parties without prior instructions from the Controller.

Art. 4: Tools and location of the data

[Provider] uses the following tools as part of its services:

Tool	Purpose	Location of the data
[RMM tool]	[Monitoring and maintenance]	[Country / region]
[EDR tool]	[Endpoint protection]	[Country / region]
[Password manager]	[Access management]	[Country / region]
[E-mail]	[Business communication]	[Country / region]
[Cloud storage]	[Administrative storage]	[Country / region]
[Backup tool]	[Backup]	[Country / region]

Transfers to servers located in the EU are covered by an adequate level of protection recognised by Switzerland, in accordance with Art. 16 FADP.

Art. 5: Security measures

[Provider] undertakes to maintain the following measures:

- Access to client systems only through a professional remote maintenance tool, with full traceability
- Encryption of client passwords through a secure password manager
- Endpoint protection through an EDR solution on all managed computers
- Keeping all tools at their latest available versions
- Access to systems limited to what is strictly necessary for the defined services

Art. 6: Incident notification

If a security incident likely to affect the practice's data is detected, [Provider] undertakes to inform the Controller as soon as possible, and at the latest within 24 hours of detection.

The notification must state at least the nature of the incident, the data potentially affected, the measures taken or envisaged and the recommendations for the Controller.

The Processor documents the incident and assists the Controller with notifying the FDPIC if necessary (Art. 24 FADP).

Art. 7: End of the agreement

At the end of the contractual relationship, [Provider] undertakes to:

- Remove all access to the practice's systems by the day after the end date at the latest
- Return or delete the passwords stored on behalf of the practice
- Return any administrative document stored on behalf of the practice
- Confirm in writing to the Controller that these measures have been carried out

Art. 8: Confidentiality

[Provider] undertakes to treat all information accessible as part of its services with strict confidentiality. This obligation applies with no time limit, including after the end of the agreement.

The Processor ensures that every person authorised to process personal data under this agreement is subject to an appropriate obligation of confidentiality.

Art. 9: Further processing by sub-processors (Art. 9 para. 3 FADP)

[Provider] declares that it uses the sub-processors listed in Art. 4 of this agreement as part of its services. This list constitutes the Controller's prior authorisation for these specific sub-processors.

Any use of a new sub-processor or any replacement of an existing sub-processor must be notified to the Controller in writing in advance. The Controller has 30 days to object. In the absence of any objection within this period, authorisation is deemed to have been granted.

[Provider] remains fully liable to the Controller for the services performed by its sub-processors. [Provider] ensures by contract that each sub-processor complies with data protection obligations equivalent to those of this agreement.

Art. 10: Right of audit

The Controller, or a third party appointed by it, has the right to check that [Provider] complies with the obligations arising from this agreement and the FADP. This check may take the form of a written questionnaire, a request for documentation or, where there are well-founded grounds, an on-site audit.

[Provider] undertakes to provide the information and documents needed for this check within a reasonable period. On-site audits are carried out during office hours, with 15 working days' notice, except in the event of a proven security incident or a request from the FDPIC, in which case no notice applies.

The costs of the audit are borne by the Controller, unless the audit reveals a failure by [Provider] to meet the obligations of this agreement.

Art. 11: Assistance with access requests (Art. 25 FADP)

If a patient or a data subject makes a request to the Controller for access to, correction or deletion of personal data, [Provider] undertakes to assist the Controller in carrying out this request, to the extent that the data concerned is accessible as part of its services.

This assistance includes searching for, identifying and, where applicable, disclosing or deleting the personal data accessible through the tools listed in Art. 4, within 10 working days of the Controller's request.

[Provider] never replies directly to a data subject. Any request received directly by [Provider] is forwarded to the Controller without delay.

Art. 12: Applicable law

This agreement is governed by Swiss law. In the event of a dispute, the courts of the canton of [Canton] have jurisdiction.

Document drawn up on the basis of the requirements of Art. 9 FADP. Having it checked by a lawyer specialising in data protection law is recommended before final contractual use.

Signatures

For the Processor	For the Controller
Name: _____	Name: _____
Role: _____	Practice: _____
Signature: _____	Signature: _____
Date: _____	Date: _____

Legal notice and terms of use

This document was written by **DentalSystems Sàrl** for information and awareness purposes. It does not constitute legal advice. The information in this document is up to date as of March 2026 and may change as legislation and regulations evolve. This English version is a translation; the French version prevails.

For any legal question relating to the FADP, the GDPR or data protection in the medical context, consult a lawyer specialising in the field.

Intellectual property

This document is the exclusive property of DentalSystems Sàrl. All of its content (texts, structure, layout and graphic elements) is protected by copyright in accordance with the Federal Act on Copyright and Related Rights (CopA, SR 231.1).

Permitted use

This template is made available free of charge. It may be modified and used under the practice's name, including with its patients, staff and providers, without keeping our references.

Prohibited use

Unless DentalSystems Sàrl has given its prior written consent, the following are prohibited:

- Selling this document, even in modified form.
- Offering it for download to third parties (download sites, sharing platforms, resellers).

The terms of use published on www.dentalsystems.ch apply; in the event of a discrepancy, they prevail over this notice.

Limitation of liability

This document is provided free of charge, for information. To the extent permitted by Swiss law, DentalSystems Sàrl is not liable for the consequences of its use; this limitation does not apply in the event of intent or gross negligence. Users remain responsible for adapting it to their situation. It replaces neither a professional audit nor legal advice.

DentalSystems Sàrl

Thomas Alvino, IT Technician

www.dentalsystems.ch | talvino@dentalsystems.ch | +41 77 245 48 44

© 2026 DentalSystems Sàrl. All rights reserved.